UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

FOR ONLINE PUBLICATION ONLY

SECURE WEB CONFERENCE CORPORATION,

Plaintiff,

- versus -

MICROSOFT CORPORATION,

Defendant.

MEMORANDUM AND ORDER

13-cv-2642

A P P E A R A N C E S:

FRIEDMAN, SUDER & COOKE
604 East 4th Street, Suite 200
Fort Worth, Texas 76102
By: Decker A. Cammack, Gregory O. Koerner, Jonathan T. Suder
Attorneys for Plaintiff

PATTERSON BELKNAP WEBB & TYLER LLP
1133 Avenue of the Americas
New York, NY 10036-6710
By: William F. Cavanaugh, Chad J. Peterman
Attorneys for Defendant

JOHN GLEESON, United States District Judge:

Plaintiff Secure Web Conference Corporation ("SWC") has brought patent infringement claims against Microsoft.[1] On September 23, 2014, I held a claim construction hearing pursuant to *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 987 (Fed. Cir. 1995) (en banc) ("*Markman I*"), *aff'd*, 517 U.S. 370 (1996) ("*Markman II*"). The case involves two patents: United States Patent No. 6,856,686 B2 ("'686 Patent"), filed on March 13, 2002,

[1] Plaintiff brought a related case, no. 13-cv-3810, against Citrix Systems, Inc., on July 9, 2013, and the briefing for this motion included both cases. However, that case was voluntarily dismissed.

describing a "Method and Apparatus for Securing E-Mail Attachments"; and United States Patent No. 6,856,687 B2 ("'687 Patent"), filed on June 5, 2002, describing a "Portable Telecommunication Security Device." Three terms in the '686 Patent and four terms in the '687 patent are disputed. I adopt some of the proposed constructions, as detailed below, and leave a few terms uninterpreted.

BACKGROUND

Both patents at issue in this case are continuations in part of U.S. Patent No. 6,430,691 ("'691 Patent"), filed June 21, 1999, for a "Stand-alone telecommunications security device." The '687 patent is also a continuation in part of the '686 patent. Both the '686 and '687 patents have listed as inventors Frank J. DiSanto and Denis A. Krusos; the '686 Patent also lists Edward Lewit. Both patent applications were filed in the first half of 2002; the patents were issued on February 15, 2005.

The case was filed on May 1, 2013. After some discovery, it was reassigned to me on June 4, 2014.

DISCUSSION

A. *Applicable Patent Law*

The claims of a patent define the patented invention. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005); *see also E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988). The claim "functions to forbid not only exact copies of an invention," but also copycat products that "go to the heart of an invention [while avoiding] the literal language of the claim by making a noncritical change." *Markman II*, 517 U.S. at 373-74 (internal citations and quotations omitted).

"An infringement analysis entails two steps. The first step is determining the meaning and scope of the patent claims asserted to be infringed. The second step is comparing the properly construed claims to the device accused of infringing." *Markman I*, 52 F.3d at 976. Construction of the claim is a legal question, and therefore the duty of the court. *See id.* at 970-71. "The construction of claims is simply a way of elaborating the normally terse claim language in order to understand and explain, but not to change, the scope of the claims." *Embrex, Inc. v. Serv. Eng'g Corp.*, 216 F.3d 1343, 1347 (Fed. Cir. 2000).

In determining the meaning of claims, courts should first consider so-called "intrinsic evidence," which includes the patent's claims, specification, and prosecution history. *See Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed.Cir. 1996); *Markman I*, 52 F.3d at 979. A claim's words should be given their ordinary and customary meaning from the perspective of a person of ordinary skill in the art at the time of the invention. *See Phillips v. AWH Corp.*, 415 F.3d at 1312-13.

The words of the claim are the controlling focus. *See Digital Biometrics, Inc. v. Identix, Inc.*, 149 F.3d 1335, 1344 (Fed. Cir. 1998). "It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips*, 415 F.3d at 1312 (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). Claims, however, must also be read in view of the specification. *See Phillips*, 415 F.3d at 1315. The United States Court of Appeals for the Federal Circuit has described the specification as "always relevant" to construction, "the single best guide to the meaning of a disputed term," and usually "dispositive." *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d at 1582). Nevertheless, case law is clear that a

patentee need not describe every conceivable and future embodiment of the invention in the specification. *See CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d at 1366.

The last piece of intrinsic evidence – the prosecution history – consists of the complete record of the proceedings before the Patent and Trademark Office ("PTO") and includes prior art cited (and distinguished) during the examination of the patent. *See Phillips v. AWH Corp.*, 415 F.3d at 1317. Neither party in this case offers prosecution history as part of its claim construction arguments.

When the intrinsic evidence does not establish the meaning of a claim, courts may also rely on other evidence – "extrinsic evidence" – including expert and inventor testimony, dictionaries, and learned treatises. *Phillips*, 415 F.3d at 1317; *see also Markman I*, 52 F.3d at 980. This evidence is useful to demonstrate how those skilled in the art would interpret the claims. *See id*. at 979. Nevertheless, extrinsic evidence is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips v. AWH Corp.*, 415 F.3d at 1317 (internal quotations omitted). The Federal Circuit has cautioned courts not to place too much reliance on extrinsic evidence and too little reliance on intrinsic sources. *See id*. at 1320. The parties rely on relatively little extrinsic evidence in their arguments before me.

B. *Terms to be Construed from the '686 Patent*

The parties seek construction of three terms from the '686 patent, all of which appear at least in its Claim 1: (1) "security device," (2) "point-to-point communications session" (or "point-to-point electronic communications session"), and (3) "security data."

1. *"Security Device"*

Plaintiff proposes that "security device" be construed as "Hardware, or a portion thereof, with a primary function of encryption/decryption." Defendant proposes "A stand-alone

telecommunications device, external to and separate from the associated microprocessor based or electronic device, capable of encrypting and decrypting data."

These competing proposals have two essential differences. First, the proposals disagree as to whether the "security device" ("SD") must be separate from and external to "microprocessor based devices" ("MBDs") mentioned in the patent. Second, the proposals disagree whether the "security device" has a primary function of encrypting and decrypting data, or whether it is merely capable of doing so. I conclude that the defendant has the better argument on both.

The claim language does not make immediately clear whether the "security device" must be physically separate from and external to the microprocessor-based devices with which it is designed to interface, and whose data it is designed to encrypt, decrypt, and transmit. But cues in the claim language hint that the "security device" is separate from those client MBDs. Initially, the very fact that the claim language employs the different terms "security device" and "microprocessor based device" implies that the entities are distinct. Furthermore, in Claim 1, SDs are described as being "associated with at least one of said plurality of microprocessor based devices." The use of the language "associated with" implies transience and separability – an impression confirmed by the claim's statement that the SD can be "associated with at least one of [a] plurality" of MBDs. It would be unnatural from that language to expect that the SD is embedded within one of those MBDs.

Similarly, Claim 8 extends the method of Claim 1 to encompass cases in which data is "sen[t]" from an MBD to an SD, encrypted in the SD, and then "sen[t]" back to the originating MBD. Although it is possible to use this terminology to describe separate parts of a single overall device, that is not the most natural inference.

In addition to the claim language, the specification provides further support for my reading that the SD is physically distinct from any MBD. In Figure 2 and its accompanying explanatory text, the specification describes a SD with "at least three input/output (I/O) ports," including ports for connecting a fax machine or phone, a port for connecting to a computer, and a port for connecting the device to an external phone line. *See id*. 3:8-20. The data port permits the security device "to be electronically coupled to any device capable of communicating with it there over, for example [] virtually any computer, personal data assistant or other proprietary device," though the specification notes that other interfaces – for example, a wireless one – could be used. *Id.* at 3:28-34. Thus, the preferred embodiment of the SD anticipates that the device can be "electronically coupled" to a wide range of MBDs, including wirelessly.

The background section of the specification also notes that "as many users already possess telephones, facsimile machines and computers, it is desirable to provide a security device capable of performing these functions in connection with these existing devices." *Id*. at 1:43-47. The purpose of the device evidently is to interface with and provide security for "existing" microprocessor based devices.

The figures in the specification also support defendant's interpretation. Figure 2, in particular, depicts the internal structure of the preferred embodiment of the SD. The figure clearly shows the SD as having two separate modems, a microcontroller, an encryption/decryption unit, and its own memory. These features enable the device to function on its own.

Finally, the '691 Patent – which both patents here in suit continue – is for a "Stand-Alone Telecommunications Security Device." This is additional evidence that the '686 SD is a physically separate entity.

In the face of this and other evidence, I find plaintiff's counterarguments unconvincing. First, plaintiff points to boilerplate language at the end of the specification:

> Although the invention has been described in a preferred form with a certain degree of particularity, it is understood that the present disclosure of the preferred form has been made only by way of example, and that numerous changes in the details of construction and combination and arrangement of parts may be made without departing from the spirit and scope of the invention as hereinafter claimed. It is intended that the patent shall cover by suitable expression in the appended claims, whatever features of patentable novelty exist in the invention disclosed.

Id. at 14:29-38. I agree with the defendant that this general language is not specifically directed to the term "security device." Moreover, based on the overall specification, it is clear that the inventor contemplated a single device that could interface with several other separate devices. Thus, the patentee's expression of generic intent that some elements could be altered without changing the overall device does not support plaintiff's construction.

Second, Secure Web makes a rather unclear argument based on language in the specification describing the "encryption/decryption device." An encryption/decryption device is shown in the preferred embodiment; it is a piece of hardware designed specifically to perform encryption and decryption. *Id*. Fig 2; *id.* at 10:32-36. The specification notes, though, that instead of using dedicated hardware, the security device could also employ its own microcontroller to perform encryption and decryption. *Id*. at 10:32-39. But none of this suggests that the "security device" is not separate from the "microprocessor based devices" with which it interfaces, and whose data it must receive, encrypt, transmit, and decrypt.

Third, Secure Web argues that Claim 3, which represents a narrowing of Claim 1, specifically contemplates a situation in which each SD is "directly electronically coupled" to an MBD. *Id*. at 14:67-15:03. But it is not clear from context what "*directly* electronically coupled"

means. It may mean something like "physically attached via short cable," which would make sense of "directly," since other language in the '686 patent makes clear that "coupled" or "electronically coupled" includes wireless connections or data connections via phone lines. *See, e.g., id*. at 15:9-12 (Claim 3, including usage that modems of each security device can be "electronically coupl[ed]"). If that is true, then Claim 1 encompasses the broader scope of situations in which the SD is connected wirelessly, or remotely over a network, to an MBD. In any event, I do not find that this argument makes plaintiff's point.

In sum, I agree with Microsoft that the term "security device" is best read to mean a device that is separate from, and external to, the "microprocessor based devices" in the claims.

Turning to the second dispute over the interpretation of "security device," I also agree with the defendant that importing a "primary function" condition into the definition is not helpful. The parties agree that the security device must, at a minimum, be capable of encryption and decryption; this is the primary means by which it can provide security. But the security device also must be able to "establish[] a point-to-point electronic communications session between" itself and another such device (each being associated with a microprocessor-based device). *See* '686 Patent at 14:48-53. Each security device must also be capable of "exchanging security data" with its mate and, once it has encrypted the data to be transferred, "transmitting [] encrypted data" to its mate. *Id*. at 14:54-61. It is not clear from this language or from elsewhere in the specification whether encryption and decryption is the "primary" one of these functions, even if it is clearly important. Thus I decline to adopt the "primary function" language.

2. *"Point-to-Point [Electronic] Communications Session"*

In the first instance, plaintiff argues that this term (which sometimes includes "electronic") needs no construction. Alternatively, plaintiff suggests "A communication between

a first microprocessor-based device and a second microprocessor-based device, during which data is exchanged." Defendant proposes "a communications session between two security devices, that is not conducted over the Internet," with the further clarification that "communications session" means "the time during which two security devices maintain a connection with each other over an uninterrupted connection." The principal disputes are whether the session occurs between MBDs or SDs, and whether a "point-to-point communications session" may include sessions conducted over the internet. Once again, I adopt defendant's construction.

First, the claims themselves make perfectly clear that the communications sessions occur between security devices, not between microprocessor based devices. For example, Claim 1 describes a method that includes "establishing a point-to-point electronic communications session between a first of said security devices being associated with a first of said microprocessor based devices and a second of said security devices being associated with a second of said microprocessor based devices." *Id.* at 14:47-53.

Second, I agree with Microsoft that the specification defines "point-to-point" as non-internet. The specification states that "Each device [] preferably also includes a permanent public/private key combination for non point-to-point transmissions, i.e. over the Internet." *Id.* at 10:53-55. While it is true that particular embodiments in the specification do not generally limit the scope of broader claim language, that is not the situation here. Here, the specification clearly articulates that "non point-to-point" communications must, at a minimum, include those conducted "over the Internet." (That is so whether "i.e." is used correctly to mean "that is," or whether it is also used to mean "for example" – because in the latter case, internet communications are at least an example of "non point-to-point" communications, even if they do

not wholly constitute the category.) It follows that "point-to-point" communications *cannot* include those conducted over the internet.

The plaintiff's citations to numerous other passages of the specification are unhelpful and confused. Briefly, the fact that the specification goes on to discuss non-realtime email file transmission does not alter the equation of "non point-to-point" with "over the Internet."[2]

3. *"Security Data"*

This term is something of a moving target. Initially, plaintiff proposes "Data used for a communications security purpose," while the defendant urges the more specific "Encryption key." But in its responsive brief, Microsoft argues that "security data" is so vague that it should be considered indefinite under the standard recently announced in *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S.Ct. 2120 (2014).

I adopt neither party's construction and leave the term partly uninterpreted for the time being. The specification and claims make clear that, at a minimum, "security data" encompasses the encryption keys used by the security devices to encrypt message data. *See, e.g.*, '686 Patent at 2:2-3 ("encrypting the data using at least the received security data"); *id*. at 14:57-58 (as part of Claim 1, "encrypting data to be transmitted using said first security device and said

---

[2] For example, the plaintiff summarizes its argument on this point in its opening *Markman* brief as follows:

> In other words, the non-point-to-point aspect as envisioned by the patentee covered the scenario in which files or emails would be exchanged over the network securely, as opposed to the "point-to-point" communications in which users communicate directly through voice, fax, or video, using any conventional communication means, including the internet.

Pl. Br. at 13 (DE 41). I agree that the specification's discussion of "non point-to-point" transmissions focuses on emailed files. The specification explains why secure transmission is more complicated when the connection is not done in realtime, because the keys used to encrypt and decrypt the files are generated anew each session and will expire if not exchanged simultaneously. *See* '686 Patent at 10:55-65. But that has nothing to do with the meaning of "point-to-point."

security data"). However, it is not entirely clear from context whether the "security data" can also include other information required to make a secure transfer.

Plaintiff argues that Claim 10 clarifies that the general usage of "security data" must be broader than just "encryption keys." Claim 10 reads: "10. The method of claim 1, wherein said security data comprises encryption key data associated with at least said second security device." *Id*. at 15:32-34. But that language is consistent with an interpretation of "security data" generally as "encryption keys associated with *both* security devices." Then Claim 10's usage would still be consistent with an interpretation of "security data" as "encryption keys."

In any event, I do not find that the record resolves the dispute. If the issue turns out to be potentially dispositive at a subsequent stage in the litigation, I will permit additional argument on the point.

For two reasons, I will also postpone consideration of the defendant's new argument that "security data" is indefinite under the Supreme Court's recent interpretation of 35 U.S.C. § 112(b) in *Nautilus*. First, there is no doubt that, by rejecting language the Federal Circuit previously employed, the *Nautilus* decision has altered the landscape for indefiniteness. But the affirmative standard that *Nautilus* intends to propound (as distinct from the previous standard) is less than clear from the decision itself. *See* 134 S.Ct. at 2129 (holding that § 112(b) "require[s] that a patent's claims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty"). The Federal Circuit will have time to interpret the decision in the coming months and offer additional (controlling) guidance on the matter. Second, because the argument was raised only in a

response, the plaintiff has not yet had an opportunity to address the impact (if any) of *Nautilus* on this case.

I note, however, that I am skeptical that the term is actually so indefinite that it fails to provide "reasonable certainty" about the meaning of the term "security data." I have already held that, from context, "security data" clearly encompasses security keys, and perhaps also includes additional data required for effecting the secure transmission of a message. This is already a fairly specific meaning.

C. *Terms to be Construed from the '687 Patent*

The parties dispute four terms in Claim 29 of the '687 patent, detailed below.

1. *"Network Communication Device"*

Plaintiff argues that this term is clear on its face and needs no construction. Defendant proposes the following: "A separate, external device, attached to a communications port on the 'device for providing secure communications over a network,' that allows for communications over the network."

Mirroring a dispute under the '686 Patent, the essential dispute here is whether the "network communications device" ("NCD") must be separate from and external to the patented "device for providing secure communications over a network" ("DSC").

I am persuaded that Microsfoft has the better argument. The language of Claim 29 supports the view that the NCD must be separate from the DSC. Claim 29 requires the DSC to have a processor capable of "selecting a configuration of a transmission and a reception port from among said communication ports dependent upon the presence of a network communication device and an input/output device in communication with said selected ports." *Id*. at 11:4-8. The "communication ports" are described above as "a plurality of communication

ports for transfer of digital data." *Id*. at 10:61-62. The reason that the processor must select an appropriate configuration of ports – that is, pick which port will receive input, and which port will send output – is because the device is designed to have a "plurality" of ports permitting a user to connect a number of different devices in different configurations. For example, a telephone port could provide either an input of data to be transmitted (for example, a voice signal) or a conduit to transmit information. That is why the configuration selected is "dependent upon the presence of a network communication device." The usage "dependent upon" further reinforces the view that each NCD is only contingently present – i.e., separate. The clear inference is that the NCDs are separate and distinct from the DSC.

Furthermore, in the context of the '687 Patent as a whole, it is clear that the DSC is a standalone, portable device capable of connecting to a multitude of different devices – wired and wireless phones, fax machines, computers – and rendering secure communications made on those devices. This is clear from the title of the patent ("Portable Telecommunication Security Device"), as well as from the "Background" section, which describes a typical use case of a business traveler or telecommuter who wishes to have secure contacts with a colleague using any of a number of possible media. *See* '687 Patent at 1:29-41. Both preferred embodiments given figures in the patent have batteries (for portability) and ports for connecting external communications devices. *See id*. Figs. 2a, 2b.

I do not adopt defendant's proposed construction wholesale, however, because of the word "attached." (Microsoft concedes in its reply that "attached" is not the best choice of words.) I believe that this term could cause confusion, since it might imply a physical connection between the NCD and DSC. Though the preferred embodiments show serial ports of the RS-232 standard (which presumably require physical connections), nothing in the claim

language restricts the connection to a physical, wired one, and the claim language is consistent with wireless connections. Indeed, the specification notes that a particular data port could be an infrared port. *See* '687 Patent at 4:48-54.

I therefore adopt the following interpretation of "network communication device": "A separate, external device, connected via a communications port on the 'device for providing secure communications over a network,' that allows for communications over the network."

2. *"Input/Output Device"*

The analysis for this term essentially duplicates the analysis above. The dispute is whether the "input/output device" must be separate: the plaintiff contends that no interpretation is necessary, while defendant seeks a construction of "A separate, external device attached to a communications port on the 'device for providing secure communications over a network' that inputs data into and receives data from the device."

The parties seem to agree that the "input/output device" and "network communication device" are either both necessarily separate from the DSC, or not. The terms appear together in the patent claims. Thus, for the reasons given above, I find that the "input/output device" is also best understood as separate from the DSC.

3. *"Selecting a configuration…"*

The parties also request construction of the following phrase (which occurs in Claims 1, 28, and 29 of the '687 patent): "selecting a configuration of a transmission and a reception port from among said communication ports dependent upon the presence of a network communication device and an input/output device in communication with said selected ports."

Plaintiff proposes interpreting only part of the phrase – "selecting a configuration of a transmission and a reception port" – with no interpretation necessary for "choosing an available port for the transmission of digital data and an available port for receiving data for encryption and transmission." By contrast, Microsoft proposes: "Selecting the port where data will be transmitted over the network dependent upon the detected presence of a network communication device and selecting the port where data is received dependent upon the detected presence of an input/output device." Furthermore, Microsoft propose that "transmission port" be interpreted as "Hardware interface where data from the 'device for providing secure communications over a network' is transmitted over the network," and "reception port" as "Hardware interface where data to be transmitted over the network is received by the 'device for providing secure communications over a network."

Though the original phrase is somewhat long and a little complicated, I do not understand this phrase to be ambiguous, and I choose not to adopt either party's construction. If this term construction turns out to matter later in the litigation, I will reconsider my decision not to construe the term.

4. *"Operable to execute code for"*

It appears that this term is not actually in dispute. Secure Web does not dispute Microsoft's proposed construction of "Capable of executing code," which makes sense in context, and is adopted.

CONCLUSION

For the foregoing reasons, the preceding term constructions are adopted.

So ordered.

John Gleeson, U.S.D.J.

Dated: October 2, 2014
Brooklyn, New York